UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/782,319	02/13/2001	Yoshiaki Kawatsura	080017.0008	9818

20457 7590 09/28/2004

ANTONELLI, TERRY, STOUT & KRAUS, LLP
1300 NORTH SEVENTEENTH STREET
SUITE 1800
ARLINGTON, VA 22209-9889

EXAMINER	
CHAI, LONGBIT	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 09/28/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/782,319	KAWATSURA ET AL.	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 April 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *13 February 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *6*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Priority

1. The application is filed on 02/13/2001 but the foreign priority has been made in this application.

2. The effective filing date for the subject matter defined in the pending claims in this application is 07/19/2000 on the benefit of foreign priority date.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1 – 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dan (Patent Number: 5825877), hereinafter referred to as Dan, in view of Bjerrum (Patent Number: EP 0402301 A1), hereinafter referred to as Bjerrum.

4. As per claim 2 and 9, Dan teaches a contents distribution method through the use of a communication network over which:

5. a recipient machine, an entitlement granter machine, and a contents distributor machine (Dan: see for example, Column 1 Line 9, Column 1 Line 49 – 51 and Column 2

Line 35 & Figure 1: An entitlement granter machine reads on an certification agency which provides the Access Control List (ACL – i.e. digital rights data) of the desired content document, the code production system reads on the recipient machines and the client system's verifier (ACL manager / enforcer) reads on the digital rights data verifier of the content distributor machine) are interconnected, comprising:

6. Dan teaches uses the digital signature along with the cryptographic hash of the ACL (digital rights data) and verify that it matches both of the signature and hash result (Dan: see for example, Column 3 Line 6 – 29).

7. Dan does not disclose expressly using the recipient's public key, putting digital signature using the entitlement granter's secret key to the thus encrypted digital rights data to create a digital signature.

8. Bjerrum teaches using the recipient's public key, putting digital signature using the entitlement granter's secret key to the thus encrypted digital rights data to create a digital signature (Bjerrum: see for example, Column 24 Line 44 – 45).

9. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Bjerrum within the system of Dan because Bjerrum teaches a method / system transferring data or electronic document which is being received in encrypted form, especially using asymmetric cryptographic techniques with a pair of key – i.e., its own private key of digital signature and other person's public key (Bjerrum: see for example, Column 3 Line 39 – 42, Column 24 Line 32 – 45).

10. Therefore, Dan as modified teaches:

a. a step to be taken on the entitlement granter machine that comprises sequential actions of encrypting digital rights data relevant to the contents request information with the recipient's public key, putting digital signature using the entitlement granter's secret key to the thus encrypted digital rights data, and sending the encrypted digital rights data with the entitlement granter's digital signature thereon to the recipient machine (Bjerrum: see for example, Column 3 Line 39 – 42, Column 24 Line 32 – 45);

b. a step to be taken on the recipient machine that comprises sequential actions of decrypting the encrypted digital rights data with the recipient's secret key and sending a message containing digital rights data thus decrypted, the encrypted digital rights data with the entitlement granter's digital signature thereon, and the recipient's public key to the contents distributor machine (Dan: see for example, Column 2 Line 66, Column 2 Line 67, and Column 3 Line 6 – 29: The imported digital rights data is the decrypted results) & (Bjerrum: see for example, Column 24 Line 44 – 45 and Column 32 Line 43 – 50: (a) Bjerrum teaches the concept using the encrypted digital rights data with the entitlement granter's digital signature thereon, to the contents distributor machine for validation and it is evident that the recipient machine just continues to pass-on this information from the source of granter machine (or CA) to the authenticity destination of contents distributor, and (b) Bjerrum also teaches a public key is widely available and known to the public and is not necessitated being sent over the network (Bjerrum: see for example, Column 32 Line 45 – 46);

c-1. a step to be taken on the contents distributor machine that comprises sequential actions of verifying the entitlement granter's digital signature by using the entitlement granter's public key (Dan: see for example, Column 3 Line 8),

11. Dan teaches verifying the hash result of digital rights data (Dan: see for example, Column 3 Line 6 – 29).

12. Dan does not disclose expressly encrypting the digital rights data with the recipient's public key, making sure that the thus encrypted digital rights data matches with the encrypted digital rights data.

13. One of ordinary skill in the art would have expected, at the time the invention was made, Applicant's invention to perform equally well with either verifying the hash result of digital rights data taught by Dan or the claimed "encrypting the digital rights data with the recipient's public key to ensure encrypted digital rights data matches with the encrypted digital rights data" because (a) both solutions perform the same function of validating the authenticity of the digital rights data (b) Bjerrum teaches an asymmetrical crypto system can be used not only for data concealment but also for authenticity purpose (Bjerrum: see for example, Column 24 Line 38 – 39).

c-2. encrypting contents data to be sent to the recipient machine with the recipient's public key, and sending the thus encrypted contents data to the recipient machine (Bjerrum: see for example, Column 3 Line 39 – 42, Column 24 Line 32 – 35, Column 24 Line 38 – 39 and Column 32 Line 43 – 50); and

d. a step to be taken on the recipient machine that is decrypting the encrypted contents data with the recipient's secret key (Bjerrum: see for example, Column 24 Line 32 – 35 and Column 32 Line 49 – 50).

e. a step to be taken on the recipient machine that is sending a message containing the recipient's public key and contents request information that the recipient wants to get specific contents to the entitlement granter machine (Bjerrum: see for example, Column 32 Line 43 – 50) & (Dan: see for example, Column 2 Line 27 – 29: The request from the recipient machines to start the entire operations is inherited from the design structures. Both Bjerrum and Dan teach a public key is widely available and known to the public and is not necessitated being sent over the network).

14. As per claim 1, 8, 15 – 16, and 18 – 19, claim 1, 8, 15 – 16, and 18 – 19 do not further teach over claim 2 / 9. Therefore, see rationale addressed above in rejecting claim 2 / 9.

15. As per claim 3 – 4, 10 – 11 and 20, Dan as modified teaches the claimed invention as described above (see claim 1 – 2, 8 – 9 and 19 respectively). Dan as modified further teaches contents distribution method comprising:

a. a step of sending an entry form for acquiring information about the recipient from the contents distributor machine to the recipient machine after the action of making sure of encrypted digital rights data matching is carried out on the contents distributor machine (Bjerrum: see for example, Column 46 Line 29 – 34: Bjerrum teaches

verification of the authenticity of the content receiving station by the content distributor is required prior to transfer electronic document to the content receiving station. It is evident this is followed after the digital rights data has been validated as taught by Dan in claim 2);

b. a step to be taken on the recipient machine that comprises sequential actions of generating an entry form filled with data as a result of that the recipient enters necessary information into the entry form, putting digital signature using the recipient's secret key to the entry form filled with data, and sending the entry form filled with data with the recipient's digital signature thereon to the contents distributor machine (Bjerrum: see for example, Column 24 Line 32 – 35, Column 24 Line 38 – 40 and Column 42 Line 49 – 54); and

c. a step to be taken on the distributor machine that comprises sequential actions of verifying the recipient's digital signature by using the recipient's public key and sending the contents data encrypted with the recipient's public key to the recipient machine (Bjerrum: see for example, Column 24 Line 38 – 40, Column 24 Line 32 – 35 and Column 3 Line 39 – 41).

16. As per claim 5 – 7 and 12 – 14, Dan as modified teaches the claimed invention as described above (see claim 1 – 2 and 8 – 9 respectively). Dan as modified further teaches contents distribution method wherein:

a. when the entitlement granter machine sends the encrypted digital rights data to the recipient machine, a certificate that is objective authentication of the entitlement

granter and includes the entitlement granter's public key is attached to the data (Dan: see for example, Column 2 Line 27);

b. when the recipient machine sends the digital rights data to the contents distributor machine, the certificate of the entitlement granter is attached to the data (Dan: see for example, Column 3 Line 5); and

c. the contents distributor machine verifies the certificate of the entitlement granter and uses the entitlement granter's public key derived from the certificate of the entitlement granter when verifying the entitlement granter's digital signature (Dan: see for example, Column 3 Line 4 – 9).

17. As per claim 17, Dan as modified teaches the claimed invention as described above (see claim 15). Dan as modified further teaches the entitlement granter machine wherein the computer system built on the entitlement granter machine is further comprised of a means to extract digital rights data that has been put under management beforehand, based on the contents request information (Dan: see for example, Column 1 Line 55 – 56 and Column 2 Line 34 – 38: Dan teaches ACL (i.e. digital rights data) is stored and extracted from the server and signed with the signature before sending to the client).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 703-305-0710. The examiner can normally be reached on Monday-Friday 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100